AKAMAI THREAT ADVISORY

2016 Holiday Shopping Advisory

Author: Benjamin Brown

Akamai
FASTER FORWARD

Issue Date: 11/22/16

Threat Advisory: 2016 Holiday Shopping Advisory

1.0 / Executive Summary / The 2016 holiday shopping season is fast approaching. More and more, shoppers are opting to make their purchases online rather than risk the frothing hordes at brick and mortar stores. With this in mind, now is a good time to review potential threats retailers digital properties may run into and what they can do about them. You will first want to get a sense of what legitimate traffic to expect and how that traffic is bound to change over time. Along with shopper traffic you will also want to prepare for potential floods of malicious traffic such as Distributed Denial of Service (DDoS) attacks, crawlers, scrapers, spammers, scalpers, account checkers, DNS hijackers, and malware pushers.

2.0 / Past Traffic Patterns and Flash Mobs / As shoppers shift to digital outlets (see figure below) it is important to take a closer look at their online shopping habits in detail. "How" shoppers are shopping isn't the only changing factor; "when" shoppers shop is also shifting. The National Retail Federation's Holiday 2015 research showed that 41 million of those consumers who shopped over the Thanksgiving weekend said they also shopped online on Thanksgiving Day itself (40%). While retailers may be focusing on Black Friday, the weekend, and Cyber Monday, it is now important that they not overlook the potential for increased traffic on Thanksgiving Day. If not, they could end up being overwhelmed by legitimate traffic they are under-equipped to serve.

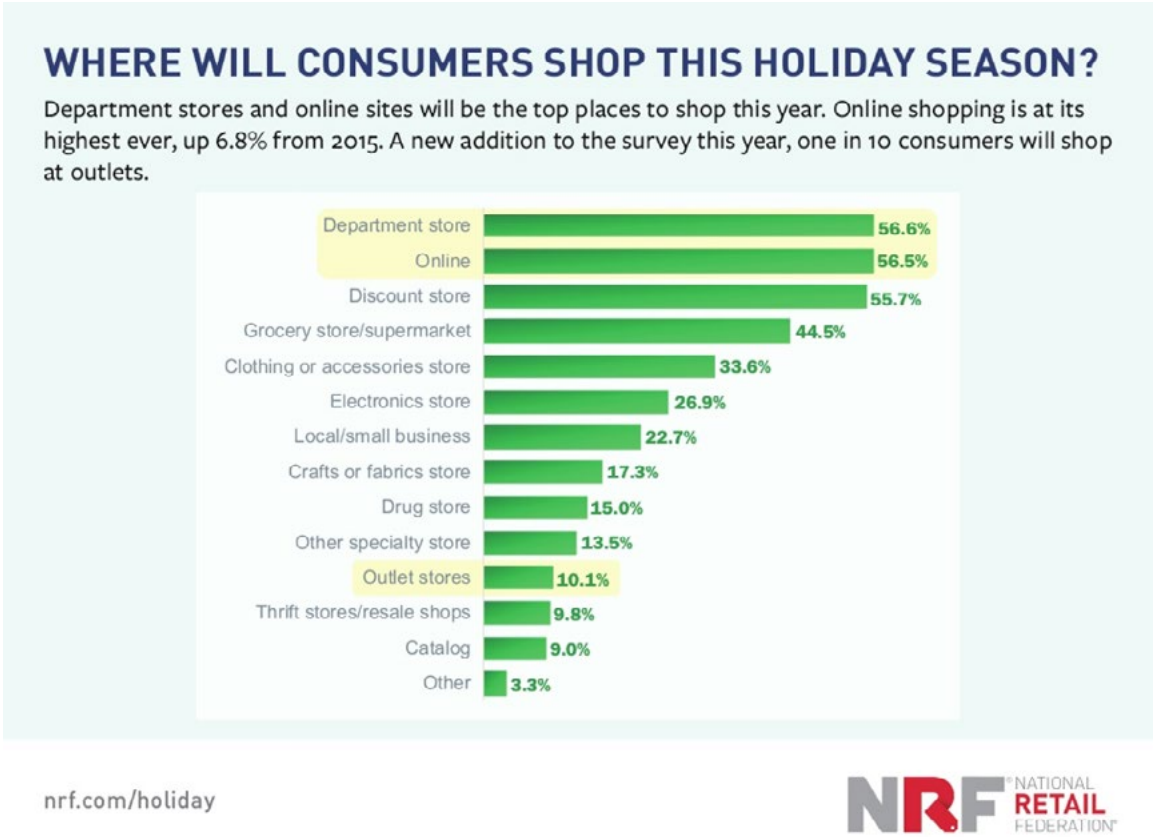

Figure 1: Retrieved Nov 2016 from https://nrf.com/resources/consumer-data/holiday-headquarters

Genuine shopper traffic doesn't always flow with a consistent or predictable pattern, so it is crucial for digital retail outlets to be prepared for flash mobs, bursts or waves of legitimate traffic that can look very similar to a DDoS attack. One way to tell the difference is to look at the ratio of clients to requests. Since a flash mob consists of human beings interacting with the digital property, there will be a relatively low number of requests and a high number of clients. In contrast, most DDoS attacks are likely to consist of a high number of requests per client with a medium to large number of clients. One way to effectively deal with flash mobs is to identify what content is likely to be highly requested and configure for efficient caching/offloading. Strategic use of static content, that flash mobs may request en mass, can also greatly reduce strain to the site. If you are an Akamai customer, you can contact your account team to assist you in evaluating and optimizing your site setup in preparation for such an event.

3.0 / DDoS/ Aside from floods of legitimate traffic, retailers should also be prepared for malicious traffic in the form of a DDoS. It could be young blackhat hackers looking to make a name for themselves, like Poodle Corp and Lizard Squad (see a screenshot of their DDoS tool below), or perhaps political activists, like Anonymous 'hacktivists'. It could be Eastern European actors retaliating for the recent attacks on Russian banks. A DDoS can also serve as a cover or distraction for the attacker's true goals such as account takeovers or data exfiltration.

A good first step in DDoS protection would be implementing a Web Application Firewall (WAF) between your website and the outside world. You will want to make sure you have the latest rule sets and review your active rules to make sure they are in alignment with your configuration and set of properties. Enforcing rate limiting rules makes sense for the type of legitimate traffic you are expecting. You may want to consider denying traffic from geographies that don't match your target consumer demographic. You may also consider blocking traffic coming through known, anonymous proxies. Plus, companies should review their current level of DNS reliability and see if a second or backup DNS provider makes sense. If the recent Dyn DNS attack showed us anything, it is that DNS centralization can lead to catastrophic scenarios. Have a play book put together ahead of time with possible attack scenarios and applicable defense maneuvers available to your team. Improve this playbook by running tabletop exercises and attack scenarios with your team. During the post-simulation review, dedicate time and effort to revising and tweaking the playbook. Iterate simulations with ever-changing variables, combine or cascade attack scenarios, and consider bringing in a professional penetration tester to refine your incident response further. Work with relevant third-party vendors to improve response times and cement clear communication protocols for system you are leveraging, but do not have complete control over.

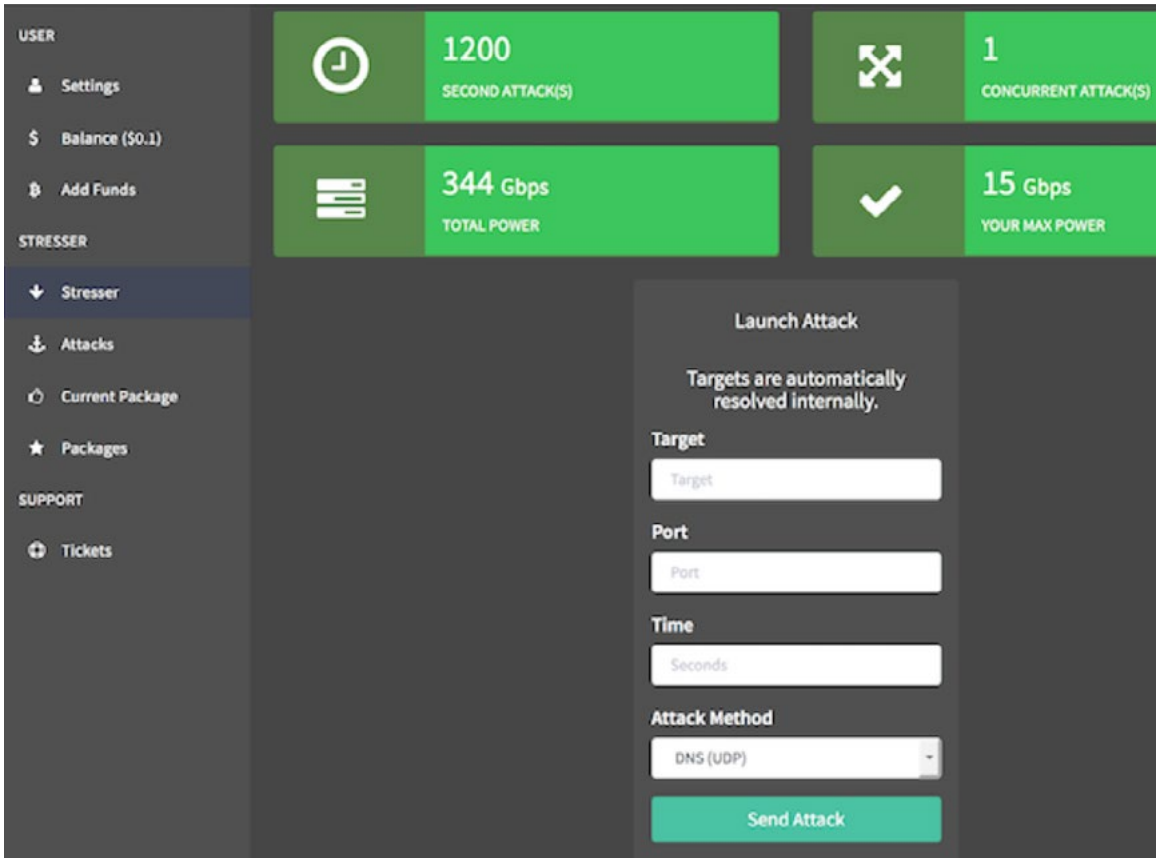

Figure 2: Interface for Lizard Squad's Shenron DDoS Tool

4.0 / Bots -"Good" Bots /

Crawlers

Much of the bot traffic that comes to your site comes in a desirable form, from search engine crawlers, such as BingBot or GoogleBot. These specific bots are tasked with crawling a page for indexing within their search engine, which in turn can direct shoppers to your website. While what they do is welcome for most retailers, they can sometimes get out of hand. It is good to know what good crawler traffic looks like (see image below), so that you can tell it apart from other traffic types, especially if that traffic starts to burst. If you are being overwhelmed with crawler traffic, search engines will typically have a webmaster portal through which you can request a change in crawler behavior. You can affect search crawler activity by directing it with a properly formatted sitemap. Additionally, a robots.txt file can be used to tell them explicitly what not to crawl. While by itself crawler traffic can seem pretty manageable, getting hammered by them while seeing massive holiday shopping traffic can make all the difference to site availability.

PATH	HTTP VERSI	METHOD	COUNTRY	ASNUM	STATUS
/shop/jewelry-watches/diamond-earrings	1.1	GET	US	26496	200
/shop/b/collared-shirt	1.1	GET	US	26496	200
/shop/womens-clothing/womens-swimwear/Swim_bottoms/Higl	1.1	GET	US	26496	200
/shop/mens-clothing/mens-shorts	1.1	GET	US	26496	200
/shop/plus-size-clothing/plus-size-sweaters/Women_plus_size_	1.1	GET	DE	24940	200
/shop/plus-size-clothing/plus-size-sweaters/Sweater_style/Crev	1.1	GET	DE	24940	200
/shop/holiday-gift-guide/gifts-we-love	1.1	GET	US	26496	200
/shop/product/alfani-plus-size-shawl-collar-knit-jacket-only-at-m	1.1	GET	DE	24940	200
/shop/plus-size-clothing/plus-size-sweaters/Brand/Alfani	1.1	GET	DE	24940	200

Figure 3: Typical Crawler Traffic

Advantageous Scrapers

There is a wide variety of scrapers, some of which actively support retail business. These automated bots are programmed to navigate to a target page and retrieve content and data to be stored and displayed elsewhere. These functions could be performed on behalf of a sales aggregator, a reseller, or a retail 'deals' portal, all able to drive additional business for the target retailer. As with any type of crawler, even desirable scrapers can become overly aggressive causing strain to the targeted digital property. Scraper traffic (example below) is pretty easy to spot and can oftentimes be used to formulate selective blocking or rate limiting to reduce the pressure on your origin. If you are able to trace the source of the traffic you can also reach out to the operator and ask them to alter their request configuration or to use an API or RSS feed you have set up for such traffic.

PATH	HTTP VERSI	METHOD	COUNTRY	ASNUM	STATUS
/shop/product/ny-collection-plus-size-roll-tab-sleeve-handkerch	1.1	GET	KR	3786	301
/shop/product/olga-flirty-back-smoothing-balconette-bra-ga471'	1.1	GET	KR	3786	200
/shop/product/oakley-sunglasses-oo4060-crosshairp	1.1	GET	KR	3786	301
/shop/product/nydj-petite-cuffed-hem-denim-shorts	1.1	GET	KR	3786	200
/shop/product/ny-collection-plus-size-ruched-a-line-dress	1.1	GET	KR	3786	200
/shop/product/ny-collection-plus-size-utility-shirt	1.1	GET	KR	3786	200
/shop/product/ny-collection-plus-size-printed-romper	1.1	GET	KR	3786	200
/shop/product/ny-collection-plus-size-short-sleeve-surplice-top	1.1	GET	KR	3786	200
/shop/product/nydj-plus-size-hayden-bootcut-jeans-dark-wash	1.1	GET	KR	3786	200

Figure 4: Typical Scraper Traffic

4.1 / Bots -"Bad" Bots /

Unwanted Scrapers

Not all scrapers have a symbiotic relationship with their retail targets. They could be operating at the behest of a competitor or a third party consultant intent on selling their analysis to others in the industry. These content scrapers could also be employed in creating a clone site for a phishing and credential harvesting campaign. Here, client reputation systems, client behavior analysis, and rate limiting can be useful tools in the fight to keep these unwanted scrapers at bay.

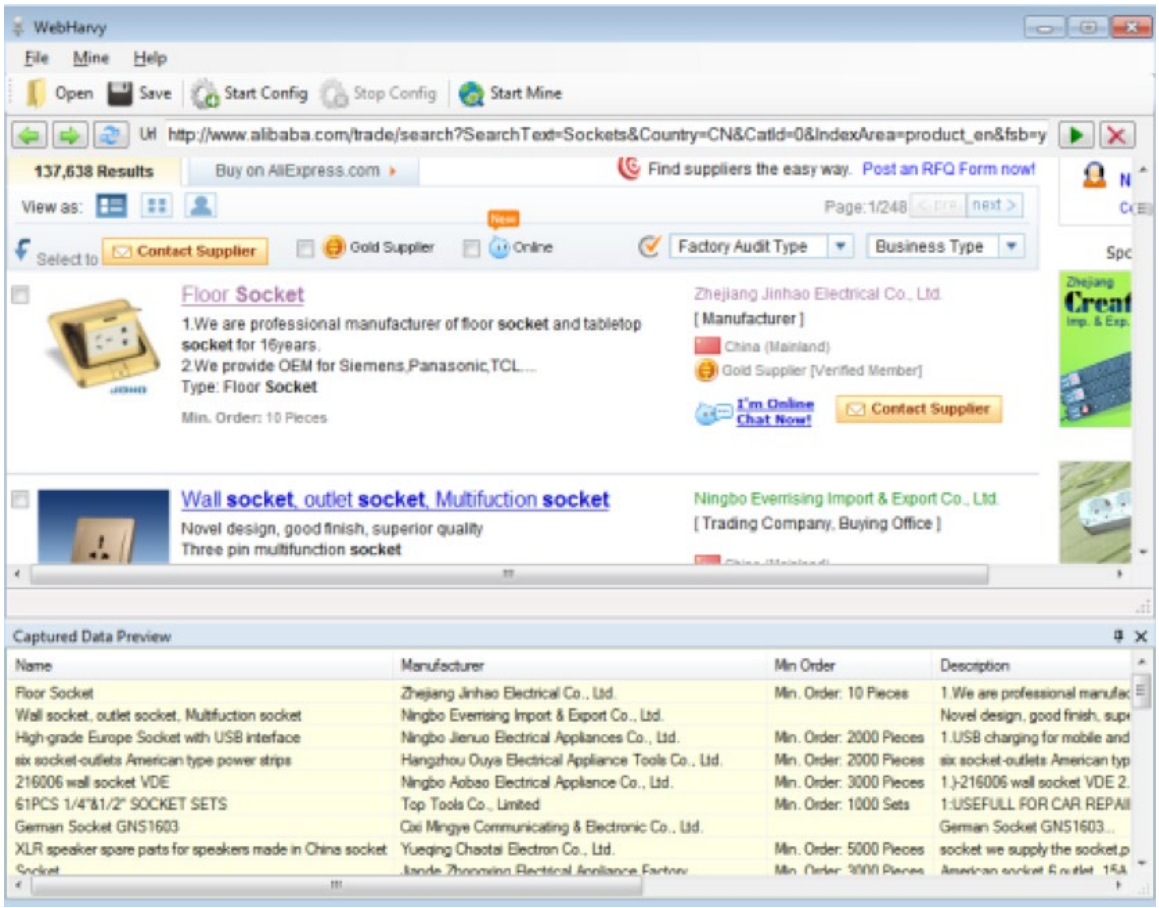

Figure 5: Professional Web Scraper Software

Spammers

Large amounts of shopping traffic to your site can make it a valuable target for spammers who want to use that popularity to get out their message. The typical M.O. is to exploit feedback, review, and customer engagement systems to publish shady links and promises of weight loss miracles, with the belief that high levels of holiday traffic will translate into a higher percentage of snared marks. It could be spam with an actual product or service on the other end, it could be a link to a phishing website, it could even be a malware download. Robust moderation, filtration, keyword analysis, and internal content review can help to stymie would-be spammers.

Scalpers

During the holiday shopping season, it is common for retailers to release limited numbers of highly sought after goods, or discount the price on these goods for a short period of time. These are the items that scalpers target using automated purchasing bots to scoop up as many as they can as fast as they can, certainly faster than any human shopper would be able to. The scalpers can then turn around and sell the targeted items at a large markup to those who were not fast enough to out click the scalpers. Common targets of this scheme are video game systems,other high-end electronics, designer watches, glasses, shoes, and bags, as well as major event tickets. We recently saw this happen with reseller price gouging of the Fallout 4 Pip-Boy Edition and the Xbox One. As with the unwanted scrapers, client reputation systems, client behavior analysis, and rate limiting are valuable defense tools.

Account Checkers

Fueled by breach after breach, account checkers are as big an issue as ever. Also known as account stuffers, these campaigns target login systems that tie into rewards or retail accounts. The highly active user base of retail websites makes the holiday shopping season prime time for these account hijackers. These accounts will typically have credit cards or loyalty points attached to them, and once criminals gain access they can use these to fuel a number of schemes. Access to active accounts can also allow crooks to reroute packages ordered by legitimate customers for either straight theft or for resale. Effective defenses here are going to include custom WAF rules fitting known account checker program fingerprints, the ability to long-route or tarpit malicious traffic (instead of just serving a 403), hunting down and closing off legacy login paths beforehand, and blocking known anonymous proxies.

In the coming months, Akamai will release a paper detailing the tools, tactics, and techniques used by these crooks. The paper will also take a peek at the underground economic lifecycle of account checker attacks.

METHOD	PATH	USER AGENT
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like ...
POST	/login/loginSubmit.do	Mozilla/5.0 (Linux; Android 5.0; SM-G900V Build/LRX21T) Apple..
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (K...
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like ...
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11..
POST	/login/loginSubmit.do	Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) Appl...
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/201001...
POST	/login/loginSubmit.do	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like ...
POST	/login/loginSubmit.do	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0) AppleWebKit/5..

Figure 6: Typical Account Checker Traffic

5.0 / DNS Hijacking and Malware Opportunities / DNS hijackers and malware droppers will also get the most out of their ploys at peaks of legitimate traffic. DNS hijacking typically involves either cracking the target domain's management account to configure a redirect, or using social engineering tactics to get the registrar to, unwittingly, make the malicious changes on the adversary's behalf. This activity has been on the rise, especially over the last four years. In 2013 and 2014 the Syrian Electronic Army (SEA) performed a number of politically motivated, high-profile DNS hijackings. 2015 saw the hijackings of Lenovo, Google Vietnam, eNom customers, and a handful of FBI seized domains, including the domain for infamous Megaupload. So far this year, Namecheap has had a bunch of customers affected by DNS hijacking. Just last month, popular Bitcoin wallet and Block Explorer service Blockchain.info were also hit by this type of attack. Once a redirect is in place, traffic intended for the legitimate retail website can now be shifted to one controlled by the hijacker to serve malware, ads, a phishing page, a political message, or any number of other sites.

To protect against DNS hijacking, make sure to employ registrar locks for domains. The first being a client lock, which helps prevent unauthenticated changes to a DNS record. The client locks include: 'clientUpdateProhibited', 'clientTransferProhibited', 'clientDeleteProhibited'. These locks won't stop changes to the DNS records if an adversary has or can get credentials to the target registrar account, as they can then log in and turn these locks off. To guard against this scenario, registrars offer server locks. These locks follow the same format: 'serverUpdateProhibited', 'serverTransferProhibited', 'serverDeleteProhibited'.

This isn't the only method available to malware pushers. Injecting their malicious code into one of the ad networks used by major retailer websites is also an option. As is the earlier mentioned use of customer interaction systems to try and fool legitimate customers into clicking risky links. Cross-site scripting, code injection, and web application vulnerabilities are also vectors for malware droppers to get the job done.

A solid and regularly updated WAF is going to be a huge asset in defending against the last three attack types. If you need to serve ads from your site, then be sure to research the ad networks you choose to partner with, look at their track record for serving malicious ads, and make sure that they have reasonable policies for who and what they accept into their network.

6.0 / Mobile and API as Targets / Mobile and API digital properties are now becoming common targets in cyber criminal campaigns as more commerce outlets are leveraging them as ways to reach a larger audience set - one that includes folks who rely in large part on mobile devices for their Internet communications and transactions. Unfortunately, go-to-market pressures often have mobile and API paths released with inadequate, or reduced, security controls when compared to the traditional site path. This makes them targets for DDoS, account checking, or data exfiltration. Make sure to perform audits of your public-facing mobile and API surface before the holiday shopping season gets here. Also, make sure there are no undocumented functions in your API setups that an outside fuzzer could discover and exploit. Finally, make sure that if one of your consumer pathways fails that the shift in traffic will not overload the remaining routes.

7.0 / Open-Source Intelligence (OSINT) / Open-source intelligence can be a great asset in both being prepared for incidents and in responding to them. Some examples of useful information an OSINT system can provide: knowing if one of your products or offers is blowing up on social media, knowing if you are listed in an attack target list, finding out if some of your user accounts are being offered for sale, getting alerted to leaked company internal or customer data.

One of the great things about OSINT is captured right in the name: "open-source." The U.S. Army Publishing Directorate defines OSINT as "Intelligence produced from publicly available information." This means that this type of processed information does not require covert human assets, membership into a secret or closed communications platform, or any sort of security clearance. This is information available through search engines, social media, news, 'paste' sites, image boards, and more.

There are some useful tools out there for obtaining and managing OSINT: Google Alerts can be configured to alert on information matching keywords of your choice. A step-up from this are the open source Scumblr and Sketchy frameworks from the Netflix security team. Scumblr allows you to create and manage automated queries to search engines and social media platforms for sites and content of interest. This data can be further manipulated or refined using Scumblr's flexible workflow processors. All this can be done through a web application-based user interface. As a companion to Scumblr, Sketchy allows you to automatically screenshot identified results to provide a snapshot of the content from when it was first identified. This in turn allows you to store and view the content without having to navigate to the site itself (especially useful if the site in question may be serving malicious content).

8.0 / Conclusion / As more and more consumers move to online shopping for the holidays, retailers have the opportunity to capitalize on lower brick and mortar expenses,and personalized shopping experiences for their customers. However, these advantages don't just require a well crafted website and workflows to attract traffic, they also require a well thought out security strategy and plan. It is imperative that information security team to work closely with web teams to predict, prepare and defend against disruptive attacks during the holiday season.